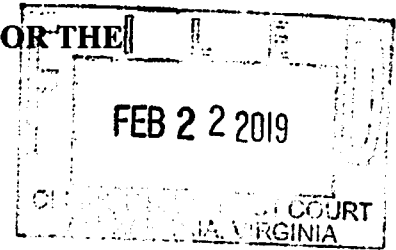


**IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA**

Alexandria Division



UNITED STATES OF AMERICA)

v.)

TIMMIE THOMAS CHATELAIN, JR.,)

Defendant.)

Case No. 1:19-MJ-98

**AFFIDAVIT IN SUPPORT OF A
CRIMINAL COMPLAINT AND ARREST WARRANT**

I, Charles Payne, being duly sworn, depose and state:

INTRODUCTION

1. I have been employed as a Special Agent of the Department of State, Diplomatic Security Service (DSS), since January 2008, and am currently assigned to the Office of Special Investigations in Rosslyn, Virginia.

2. While employed by DSS, I have investigated federal criminal violations related to child exploitation and child pornography. I have received training in the area of investigating child pornography and child exploitation crimes and have had the opportunity to observe and review numerous examples of child pornography, as defined in 18 U.S.C. § 2256(8), including computer media. Due to my experience and training, I can identify child pornography when I see it. I have training and experience in the enforcement of the laws of the United States, including the preparation, presentation, and service of subpoenas, affidavits, criminal complaints, search warrants, and arrest warrants.

3. This Affidavit is made in support of a criminal complaint and arrest warrant charging **TIMMIE THOMAS CHATELAIN, JR.** with knowingly transporting child pornography using any means or facility of interstate commerce in violation of Title 18, U.S. Code, Sections 2252(a)(1) and (b)(1).

4. I am familiar with the information contained in this Affidavit based upon the investigation I have conducted, along with my conversations with law enforcement officers and others and the review of reports, database records, and other materials. This Affidavit is submitted for the limited purpose of supporting a criminal complaint and securing an arrest warrant. It does not include each and every fact known to me or the government about the investigation. I have set forth only those facts that I believe are necessary to establish probable cause to believe that **CHATELAIN** knowingly transported child pornography.

INFORMATION REGARDING APPLE ID AND iCloud

5. Apple is a United States company that produces, for example, the iPhone and iPad, which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications.

6. Apple iCloud is a cloud-based file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and

iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents.

7. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

8. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail).

DETAILS OF THE INVESTIGATION

9. On December 7, 2018, the Department of State, Diplomatic Security Service, Office of Special Investigations, received information regarding potential child pornography found on a United States government owned laptop (hereinafter “the Laptop”) at the United States Embassy, Bangui, Central African Republic (hereinafter “Embassy”). The Laptop is shared device, used by Embassy employees without sign-in or sign-out procedures. The Embassy’s Information Management Officer (“IMO”) and the staff of the Embassy Information Management Section are the administrators of the Laptop and have access to its administrative function. At this stage of the investigation, your affiant does not know the full extent of individuals who have access to the laptop or its specific user accounts.

10. According to the information received, while using the Laptop in the course of his employment, a staff member at the Embassy came across what he referred to as “pedophilia contents” on the Laptop in a user account that had administrative privileges—meaning once an

individual signs into that account, they would be able to download programs from the internet onto the Laptop. The employee notified the IMO, who then informed the Embassy Regional Security Officer Specialist Special Agent Christopher Good. Special Agent Good secured the Laptop.

11. On December 21, 2018, the Laptop was transferred to the custody of an Assistant Regional Security Officer Special Agent, who delivered it to your affiant at Dulles Airport on December 22, 2018. Your affiant secured the Laptop at a Department of State office located in Rosslyn, Virginia, in a bar-locked, combination container.

12. The Laptop was subsequently transferred to the Diplomatic Security Computer Investigations and Forensics Division, and a forensic analysis was conducted. The analysis concluded that the Laptop has a Microsoft-based operating system.

13. The analysis further revealed that on October 4, 2018, the Apple iCloud application was installed on the Laptop. Once downloaded, this application sets up an iCloud Drive folder on the user's device that can be accessed in a similar manner to other computer folders. This allows a user to access the files and documents in their iCloud account at any time, and, when internet-connected, changes made to the iCloud on any other device will be reflected in the iCloud Drive folder.

14. On October 22, 2018, the user of the Laptop logged into the administrative account "dosadmin" and either re-downloaded or updated the iCloud application. The user of the Laptop then navigated to the webpage of the State Department Federal Credit Union Bank ("SDFCU"). Membership with SDFCU is limited to State Department employees and employees or affiliates of groups approved by SDFCU. Generally, local Embassy employees are not eligible for SDFCU membership.

15. The user of the Laptop then changed the password associated with the DOSAdmin account. After logging in with these new credentials, the user of the Laptop downloaded the contents of a specific iCloud account onto the laptop. The login credentials for the downloaded account were “timchatelain@mac.com.”

16. The contents of the iCloud account downloaded to the Laptop included hundreds of images of child pornography and child erotica. The iCloud folder structure contains a folder titled “Desktop” and within this folder there are additional folders including “Desktop Pic’s” and “desktop doc’s 2.” The dates associated with the child pornography and child erotica images indicate that such files were added to the iCloud account beginning in at least September 2017 and continuing through at least May 2018. Those images include:

- a. “sm-88-Ap-JL-32.jpg”: This image depicts a prepubescent female being vaginally penetrated by an adult penis. This file was in sub-folders within “Desktop Pic’s” folder.
- b. “sm-41482332HGL.jpg”: This image depicts a prepubescent male being orally penetrated by an adult penis. This file was in sub-folders within “Desktop Pic’s” folder.
- c. “Foiijhasoigj.jpg”: This image depicts a prepubescent female being orally penetrated by an adult penis. This file was in sub-folders within “Desktop Pic’s” folder.
- d. “yMrc5s6.jpg”: This image depicts a female infant or toddler laying on an open diaper while an adult hand inserts an unidentifiable object into the child’s vagina. The image contains text in the corner which reads “Kiddielover Collection.” This file was in a sub-folder within “Desktop Pic’s” folder.

- e. “thumb_06257.jpg”: This image depicts a prepubescent female being vaginally penetrated by an adult male. This file was in the “Desktop Pic’s” folder.

17. Many of these files, as well as many of the other files in the iCloud Drive, are stored in a format that appears to be webpage images from webpages viewed by the user. Additionally, some of the child pornography files were saved in a format called “webarchive.” Webarchive files are generated when a user saves versions of webpages using the Apple Safari web browser. This allows the user to later view the webpage, even when not connected to the internet.

18. The forensic analysis showed that, in addition to the Laptop, an Apple MacBook Pro, a Kingston portable storage device, and an Apple iPhone had been used in connection with the iCloud account.

19. Results of the forensic analysis show that the iCloud account is associated with **CHATELAIN**. The Apple iCloud account is associated with the username(s) **timchatelain@mac.com**. Additionally, contents of the iCloud folder downloaded to the laptop contain several documents associated with **CHATELAIN**, including airline flight itineraries, bank account records, investments, cover letters and draft documents referencing bank wire transfers, email account information, a copy of the page of his diplomatic passport showing his photograph and identifying information, and personal photographs. Some of these documents containing **CHATELAIN’S** information are stored in the same folder as child pornography. In particular, the folder “desktop doc’s 2” contains multiple images that appear to be child pornography or child erotica. Also contained within this folder are documents with **CHATELAIN’S** name and person information, including personal airline flight itineraries, cover

letters and draft documents referencing bank wire transfers, documents referencing real estate transactions, personal email account information, State Department-related files.

20. Your affiant identified **CHATELAIN** in the personal photographs contained within the iCloud folder based on a comparison to his passport photograph. The contents also included an Excel spreadsheet, saved as an attachment to emails found within a container file holding a collection of email messages, with dozens of usernames and passwords for various accounts, including **CHATELAIN'S** Department of State account. Many of the usernames in the spreadsheet include a variation on **CHATELAIN'S** name, such as "CHATELAINTT", "Tchatelain", and "timchatelain".

21. **CHATELAIN** is a United States citizen and a Department of State retired annuitant, also known as "While Actually Employed" (an employee permitted to work up to six months a year). **CHATELAIN** works as an Information Management Officer at the United States Embassy Bangui, Central African Republic. He most recently worked at the Embassy from August 31, 2018 until November 9, 2018, and was therefore working at the Embassy and had access to the Laptop when the iCloud account timchatelain@mac.com was downloaded to the Laptop.

22. The investigation showed that **CHATELAIN** was scheduled to travel from Honolulu, Hawaii to Reagan National Airport via Atlanta, Georgia. **CHATELAIN** was scheduled to arrive at Ronald Reagan National Airport on February 21, 2019. **CHATELAIN** was scheduled to attend a Department of State training course from February 25 through March 1, 2019 in West Virginia.

23. As described above, an iCloud account can be accessed by any device that has internet access capability, including computers, laptops, and cell phones. The forensic analysis

showed that the iCloud account timchatelain@mac.com has been accessed from a variety of devices, both Apple devices and non-Apple devices. In addition to being downloaded onto the Laptop, which was running a Microsoft operating system, the timchatelain@mac.com account was connected to a non-Apple storage device and two Apple devices. Collectively, these devices span a variety of types of electronic media, including laptop computers, cell phones, and removable storage devices. The iCloud account belonging to **CHATELAIN** contains hundreds of images of child pornography and child erotica, saved to the iCloud account on multiple dates over the course of at least a year. Additionally, the account contains many other personal items belonging to **CHATELAIN**, including information regarding bank accounts, wire transfers, and personal photographs.

24. Based on the above, a search warrant was obtained in the Eastern District of Virginia on February 19, 2019. The search warrant authorized the United States to seize and forensically search any electronic devices that **CHATELAIN** had in his possession or on his person when he arrived at Reagan National Airport on February 21, 2019.

25. On February 21, 2019, **CHATELAIN** arrived at Reagan National Airport in Arlington, Virginia, within the Eastern District of Virginia, on a flight that had originated in Atlanta, Georgia. DSS agents approached **CHATELAIN** at baggage claim and identified themselves as law enforcement.

26. **CHATELAIN** had in his possession an iPhone, two MacBook laptops, a MacBook Air laptop, three thumb drives, and two hard drives.

27. An initial review was performed on the Seagate 1TB external USB hard drive (serial number NA96F6L4) recovered from one of **CHATELAIN'S** bags. That review found multiple images of child pornography, including the following:

- a. “1.jpg”: This image depicts a prepubescent minor, on her arms and knees, exposing her anus and genitalia. What appears to be an erect adult penis is also in the image.
- b. “486441.jpg”: This image depicts a prepubescent male minor and a prepubescent female minor, both fully nude. The female minor is touching the male minor’s penis with her hand.
- c. “y3ApRSD.jpg”: This image depicts a prepubescent female minor, fully nude, with her legs spread and her genitalia exposed. Her hand is touching an adult penis.
- d. “sm-41482332HGL.jpg”: This image depicts a prepubescent male minor being orally penetrated by an adult penis.
- e. “sm-Vindt_het_zo_te_zien_lekker.jpg”: This image depicts a prepubescent female minor, nude, on her hands and knees, being vaginally penetrated by an adult penis.

//

//

//

//

//

//

//

//

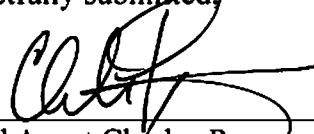
//

//

CONCLUSION

24. For the foregoing reasons, I submit to the Court that probable cause exists to believe that **TIMMIE THOMAS CHATELAIN** has knowingly transported child pornography using a means or facility of interstate commerce in violation of 18 U.S.C. §§ 2252(a)(1) and (b)(1). I, therefore, respectfully request that the Court issue a criminal complaint.

Respectfully submitted,



Special Agent Charles Payne
Diplomatic Security Service
U.S. Department of State

Subscribed to and sworn to before me
on this 22 day of February, 2019.

/s/
Michael S. Nachmanoff
~~United States Magistrate Judge~~
The Honorable Michael S. Nachmanoff
United States Magistrate Judge
Alexandria, Virginia